# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-215242
(43)Date of publication of application : 11.08.1998

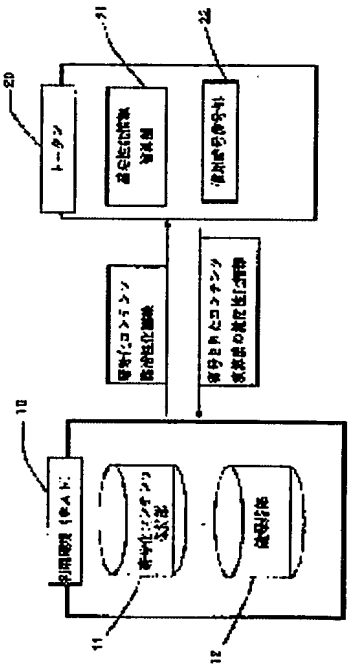
(51)Int.Cl. H04L 9/08
G06F 15/00
G06F 17/60
G09C 1/00
H04L 9/14
// G06F 12/14

(21)Application number : 09-016085
(22)Date of filing : 30.01.1997

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : KIKO KENICHIROU
SAITO KAZUO

## (54) AUTHENTICATION METHOD AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To execute the control of utilization sequence of enciphered contents in off-line.
SOLUTION: In the case of using a first key, a corresponding key is retrieved from a key storage section 12 based on an ID imparted to contents. A value of a field denoting a remaining number of times corresponding to the key in the key storage section 12 and when the value is zero, a host 10 sends the contents and the key to a token 20. A decoding section 22 of the token 20 uses the key to decode the contents and sends the result to the host 10. The host 10 checks an ID of a key used next to the present key from the key storage section 12. When the ID of the next key is not zero, the host 10 retrieves the next key based on the ID and conducts key activation processing when the corresponding key is found out. When the ID of the next key is zero, since the next key is not in existence, no key activation processing is conducted. The host 10 utilizes the decoded contents.



LEGAL STATUS

| | |
|---|---|
| [Date of request for examination] | 04.07.2001 |
| [Date of sending the examiner's decision of rejection] | 14.12.2004 |
| [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | |
| [Date of registration] | |
| [Number of appeal against examiner's decision of rejection] | 2005-00690 |
| [Date of requesting appeal against examiner's decision of rejection] | 12.01.2005 |
| [Date of extinction of right] | |

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－215242

(43)公開日　平成10年(1998)８月11日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/08 | | Ｈ０４Ｌ | 9/00 | ６０１Ｂ |
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ｚ |
| | 17/60 | | Ｇ０９Ｃ | 1/00 | ６６０Ｂ |
| Ｇ０９Ｃ | 1/00 | ６６０ | Ｇ０６Ｆ | 12/14 | ３２０Ｂ |
| Ｈ０４Ｌ | 9/14 | | | 15/21 | Ｚ |

審査請求　未請求　請求項の数15　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平9－16085

(22)出願日　平成９年(1997)１月30日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　斉藤　和雄
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

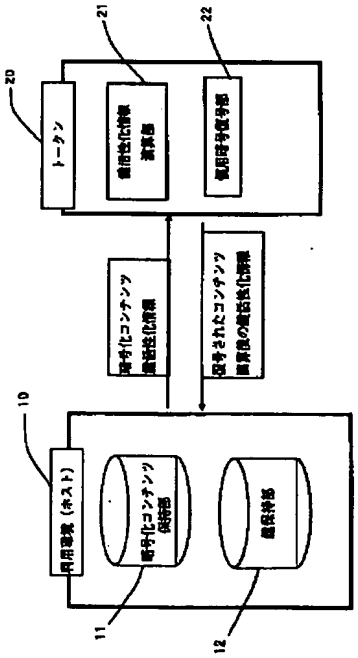
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　認証方法および装置

(57)【要約】

【課題】　暗号化されたコンテンツの利用順序の制御をオフラインで実施できるようにする。

【解決手段】　最初の鍵を使用する際にはコンテンツに付与されたＩＤを基に対応する鍵を、鍵保持部１２より検索する。鍵保持部１２の鍵に対応する残り回数のフィールドの値を調べ、値が０の場合にはホスト１０はトークン２０にコンテンツと鍵を送る。トークン２０の復号部２２は鍵を利用してコンテンツを復号しホスト１０に送る。ホスト１０は、鍵保持部１２から、現在の鍵の次に使用できる鍵のＩＤを調べる。次の鍵のＩＤが０でない場合、ＩＤをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う。次の鍵のＩＤが０の場合には、次の鍵は存在しないので、鍵活性化処理は行わない。ホスト１０は、復号されたコンテンツを利用する。



1

【特許請求の範囲】

【請求項１】　異なる認証を所定の順序で行う認証方法において、
先順序の認証のために対応する先順序の証明情報を利用するステップと、
上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、
上記後順序の認証のために上記後順序の証明情報を利用するステップとを有することを特徴とする認証方法。

【請求項２】　順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列を利用して上記証明情報に対応した認証を行う認証方法において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしたことを特徴とする認証方法。

【請求項３】　複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項２記載の認証方法。

【請求項４】　証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項２記載の認証方法。

【請求項５】　順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先である証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしたことを特徴とする証明情報生成方法。

【請求項６】　複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにした請求項５記載の証明情報生成方法。

【請求項７】　利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにした請求項５記載の証明情報生成方法。

【請求項８】　特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置であって、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段を有することを特徴とするユーザ認証装置。

【請求項９】　一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにすることを特徴とする暗号鍵利用順序制御方法。

【請求項１０】　複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成される請求項９記載の暗号鍵利用順序制御方法。

【請求項１１】　暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成される請求項９記載の暗号鍵利用順序制御方法。

【請求項１２】　一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしたことを特徴とする暗号鍵生成方法。

【請求項１３】　複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項

１２記載の暗号鍵生成方法。

【請求項１４】　利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項１２記載の暗号鍵生成方法。

【請求項１５】　暗号化されたデジタル情報を復号して利用するための復号装置であって、復号鍵によって当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段を有することを特徴とした復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の認証を所定の順序で行う認証技術に関し、その順序を逸脱した場合には認証が正しく行われないようにしたものである。また本発明は、先の順序の証明情報を利用することにより暗号化されたデジタル情報を復号して利用する場合の、暗号鍵の生成方法に関し、あらかじめ定められた順序に従ってデジタル情報を特定の回数利用することにより、次に定められた暗号鍵が生成される技術に関する。

【０００２】なお、本発明の利用範囲はコンテンツを暗号化して流通させ、その利用順序を制御するだけにはとどまらず、一般に暗号鍵（署名のための鍵、検証のための鍵など、暗号技術における鍵、一般）の利用順序の制御を可能とするものである。

【０００３】従って例えば、電車の乗車券や映画の鑑賞券のようなチケットを電子的に発行する場合に、乗車券はキセルを防ぐために予め決められた順序でしか乗車券を使えないようにしたり、あるいはある映画を見ると別の映画を安く見ることができるなどの鑑賞券の売り方を実現する際にも、電子的に発行されたチケットの利用順序の制御にも適用することが可能である。

【０００４】

【従来技術】近年のネットワークの発達により様々な情報がデジタル化され、流通するようになってきている。デジタル情報は複写が容易であり、複写されたものは劣化しないという特質があるため、金銭的な価値を持つデジタルコンテンツ（画像、動画、プログラムなど）を暗号化して流通させ、使用時にユーザの環境で復号して利用するという流通形態が開始され始めている。ＮＴＴ社のｍｉＴａＫａＴＴａ（商標）や、ＩＢＭ社のＩｎｆｏｍａｒｋｅｔ（商標）が現在実施されている代表的なサービスである。コンテンツが共通の鍵で暗号化されて配布される場合には、一旦鍵が露呈するとその鍵が流布することによってコンテンツがただで利用されてしまうという問題がある。そこで、これらのサービスではコンテンツを利用する時にのみ、オンラインで一時的に鍵を配布し、利用が終わると鍵は捨てられるように構成されている。



【０００５】しかし、この構成ではコンテンツの利用がオンラインでしかできないことになり、ユーザに対して通信コストの負担不便を強いることになる。

【０００６】一方、それに対して特公平６－９５３０２号公報のソフトウェア管理方式や、ＷａｖｅＳｙｓｔｅｍ社の開発したＷａｖｅＣｈｉｐ（商標）などの技術では、コンテンツは予め決められた暗号鍵で暗号化されて流通させ、利用者はそれを復号するための共通の鍵の封入されたＩＣカードあるいはＩＣチップを自分のＰＣに接続し、利用したいときはその装置内で復号してコンテンツを利用するというような形態により構成している。ＩＣカードなどのデバイス内では利用するごとに履歴が取られ、後でその履歴に応じて料金を徴収するというものであった。

【０００７】しかし、この方法によるとユーザの資格などに応じて、利用可能なコンテンツを制限したりすることは不可能であった。

【０００８】そこで、本出願人はあらたなユーザ認証技術を提案している（特願平９－４１８号）。この提案によれば、コンテンツは共通の鍵で暗号化し、ユーザは自分自身の鍵を持ち、アクセスチケットと呼ぶコンテンツとユーザの間を取り持つためのチケットを導入することで、暗号化されたコンテンツのオフラインでの利用を可能とし、さらにユーザ毎にアクセスチケットの発行をコントロールして、アクセス制限を行うことを可能としている。

【０００９】

【発明が解決しようとする課題】しかしながら、特願平９－４１８号の提案によると、コンテンツを利用するためのアクセスチケットはそれを発行可能であるコンテンツの配布者あるいはチケット発行センターのような機関に依頼せねばならない（以下、簡単のためこれらを総称してセンターと呼ぶ）。すなわち、ユーザはアクセスチケットを一旦手に入れてしまえばオフラインで使い続けることが可能となるが、新たなコンテンツを利用しようとした場合には前記センターにオンライン（あるいはそれに代わる手段）で依頼しなければならないことになる。

【００１０】予め幾つかの部分に分割され、それらが順序だてて利用されることを想定して作られたコンテンツ、例えば小説や物語、段階を追って難しくすることを意図した問題集などでは、これらのコンテンツは部分に分割され、それぞれの部分ごとに異なった暗号化が施さ

れ、それぞれ利用する際には異なるアクセスチケットを要求するように構成される。

【００１１】しかし、コンテンツの利用順序を限定しようとするためには、センターはユーザに対して一括してアクセスチケットを発行することはできないため、ユーザは新たな部分を利用したいと思う度にアクセスチケットを手に入れるためにセンターに発行を依頼しなければならないことになる。

【００１２】また、利用順序が線形でなく、二つの異なったコンテンツを順序に関わりなく利用することにより、別のコンテンツが利用可能になるという、提供方法もある。このような販売形態を採ろうとすると、従来の方法では、やはりユーザは三つ目のコンテンツを利用するためのチケットをセンターに発行依頼しなければならない。

【００１３】

【発明が解決しようとする課題】本発明は上記のような問題に鑑みてなされたものであり、その目的とするところは、ユーザによる暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御をオフラインで実施可能であるようにすることにある。

【００１４】

【課題を解決するための手段】まず、本発明の概要について具体的な実現環境に即して説明する。本発明の１実現環境では、上記の課題を解決するため、ユーザ環境をコンテンツの利用環境と、あらかじめユーザ毎に配られるトークンによって構成する。トークンはＩＣカードなどの演算機能を持つ耐タンパー容器である。そして、ある鍵に対して特定の演算を複数回繰り返す事で、始めて次に指定された鍵が生成されるように計算された複数の鍵を発行し、ユーザ環境においてトークンがこの定められた演算を行った結果を基にして、次の鍵を生成することで次の鍵が利用可能になる。

【００１５】また、本発明は上記の課題を解決するため、アクセスチケットを用いたアクセス制御方法（特願平９－４１８号）において、一連の複数のチケットとそれぞれのチケットに対応する利用制限情報をあらかじめ決められた計算方法に基づいて発行する。アクセスチケットの利用制限情報には、このチケットの使用順位もしくは次に使用するチケットを識別する数値、次のチケットを使用可能にするためのチケット活性化情報、次のチケットが使用可能になるまでの回数、及び次のチケットの法数のフィールドが含まれる。そして、発行した複数のチケットと、最初に用いるチケットに対応する利用制限情報のみをユーザに配布する。

【００１６】あるチケットの次のチケットを使用可能にするためのチケット活性化情報は、現在使用しているチケットを用いて、トークンとの間で定められた回数の通信を行う事でのみ生成される。こうして生成されたチケット活性化情報を、次に使用するチケットの利用制限情報の特定のフィールドに追加する事により、はじめて次のチケットが使用可能になる。



【００１７】次のチケットは異なるコンテンツに対するものであってもよいし、同一のコンテンツに対して、異なる利用条件での使用を許可するものであってもよい。

【００１８】さらに、本発明の構成について詳細に説明する。

【００１９】本発明によれば、上述の目的を達成するために、異なる認証を所定の順序で行う認証方法において、先順序の認証のために対応する先順序の証明情報を利用するステップと、上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、上記後順序の認証のために上記後順序の証明情報を利用するステップとを実行するようにしている。

【００２０】この構成においては、先順序の証明情報を実際に使用して初めて後順序の証明情報が利用可能になり、認証を所定の順番で行うように強制できる。

【００２１】また、本発明によれば、上述の目的を達成するために、順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列の利用して上記証明情報に対応した認証を行う認証法補において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしている。

【００２２】この構成においては、先の証明情報が利用されて、後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００２３】また、この構成において、複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【００２４】また、証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【００２５】また、本発明によれば、上述の目的を達成するために、順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先であ

る証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしている。

【００２６】この構成においても、先の証明情報が利用されて、後の証明情報が生成されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００２７】また、この構成において、複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【００２８】また、利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【００２９】また、本発明によれば、上述の目的を達成するために、特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置でおいて、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段とを設けるようにしている。

【００３０】この構成においても、先の証明情報が利用されて後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００３１】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにしている。

【００３２】この構成においては、複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成されるようにしてもよい。

【００３３】また、暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成されるようにしてもよい。

【００３４】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしている。

【００３５】この構成においては、複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよいまた、利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。

【００３６】また、本発明によれば、上述の目的を達成するために、暗号化されたデジタル情報を復号して利用するための復号装置に、復号鍵によって、当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段とを設けるようにしている。

【００３７】この構成においては、先行する復号鍵を利用することにより後続の復号鍵を活性化させることで可能となり、予め定められた順序で復号を行うことが可能となる。

【００３８】

【発明の実施の態様】以下、本発明の実施例について説明する。

【００３９】［実施例１］本実施例では、１つの暗号化

鍵を特定の回数用いる事により、異なるコンテンツに対する暗号化鍵を生成する方法について述べる。

【００４０】本実施例は、デジタルコンテンツを暗号化して鍵と共に提供するコンテンツプロバイダと、提供されたコンテンツを復号して利用するためのユーザ環境とからなる。

【００４１】図１は、ユーザ環境を示しており、この図において、ユーザ環境は、利用環境（ホスト）１０とトークン２０とからなり、利用環境１０は暗号化されたデジタルコンテンツを保持するコンテンツ保持部１１と、それに対応する鍵を保持する鍵保持部１２とを含んで構成されている。トークン２０はあらかじめユーザ毎に配布される、スマートカードやＩＣカードであり、鍵を活性化させるための演算部２１とコンテンツ、もしくはコンテンツを復号するための情報を復号するための復号部２２を持つ。

【００４２】次に実施例の動作について図２および図３を参照して述べる。図２は実施例の全体的な処理を示す。図３は鍵活性化処理の詳細を示す。

【００４３】なお、本実施例では、コンテンツプロバイダは４つの異なるコンテンツが順番に利用されるように、鍵を発行する。始めにコンテンツプロバイダは、コンテンツを慣用暗号鍵Ｋ１で暗号化する。さらに、他のコンテンツを、利用する順番にそれぞれＫ２～Ｋ４の鍵で暗号化する。そして、以下のように、Ｋ２’～Ｋ４’を計算する。

【００４４】

【数１】Ｋ２’＝Ｋ２－$F^{Ur2}$（Ｋ１）

Ｋ３’＝Ｋ３－$F^{Ur3}$（Ｋ２）

Ｋ４’＝Ｋ４－$F^{Ur4}$（Ｋ３）

$F^{Ur2}$（Ｋ１）はＫ１に対してＦの演算をＵｒ２回繰り返す事を意味している。

【００４５】Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、Ｕｒは次のチケットを使用可能にするために現在のチケットを使用しなければならない回数である。Ｆの計算方法を秘密とし、ユーザ毎にその計算方法を異なるものとすれば、他のユーザが計算した値を流用される事はない。ユーザには、Ｋ１とＫ２’～Ｋ４’および、Ｕｒ２～Ｕｒ４が配布される。ユーザに配布された鍵は鍵保持部１２に保持される。一連の鍵が配布された時点での、鍵保持部１２の様子を図４に示す。

【００４６】さて、図２において、最初の鍵を使用する際にはコンテンツに付与されたＩＤを基に対応する鍵を、鍵保持部１２より検索する（Ｓ１０）。対応する鍵が無い場合は処理を終了する（Ｓ１１）。次に、鍵保持部１２の鍵に対応する残り回数のフィールドの値を調べ、値が０でない場合はその鍵はまだ有効ではないので、やはり処理を終了する（Ｓ１２）。ホスト１０はトークン２０にコンテンツと鍵を送る（Ｓ１３）。トークン２０の復号部２２は鍵を利用してコンテンツを復号しホスト１０に送る（Ｓ１４）。ホスト１０は、鍵保持部１２から、現在の鍵の次に使用できる鍵のＩＤを調べる（Ｓ１５）。次の鍵のＩＤが０でない場合、ＩＤをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う（Ｓ１６～Ｓ１９）。次の鍵のＩＤが０の場合には、次の鍵は存在しないので、ホスト１０は復号されたコンテンツを利用する（Ｓ２０）。

【００４７】次に図３を参照して鍵活性化処理Ｓ１９について詳細に述べる。図３において、鍵活性化処理では、まず鍵保持部１２から鍵に対応する鍵活性化情報を取得する（Ｓ２１）。この値が０であった場合には、鍵活性化情報のフィールドに、現在の鍵の値を書き込む（Ｓ２２、Ｓ２３）。次に、ホスト１０はトークン２０に現在の鍵活性化情報αを送る（Ｓ２４）。トークン２０はＦ（α）を計算しホスト１０にその値を返す（Ｓ２５）。鍵保持部１２の、次の鍵の残り回数Ｕｒの値（図４）を１減らす（Ｓ２６）。１減らした結果、残り回数Ｕｒの値が０にならない場合には、ユーザ環境はＦ（α）の値で、現在の鍵の活性化情報を置き換える（Ｓ２７、Ｓ２８）。値が０になった場合には、次の鍵の値にＦ（α）を足したもので、次の鍵の値を置き換える（Ｓ２９）。このようにして２番目の鍵が使用可能になった時点での、鍵保持部の様子を図５に示す。これで、鍵活性化処理は終了し、ホスト１０は復号されたコンテンツを利用する。

【００４８】このように一連の鍵を上記のような方法で、関連付けて作成する事により、第一の鍵Ｋ１を特定回数使うことにより、初めて、第二の鍵Ｋ２を計算する事ができ、これにより第二の鍵Ｋ２が利用可能になる。同様の処理により、順次異なる鍵を、定まった順序・回数でのみ利用する仕組みが実現できる。

【００４９】［実施例２］本実施例では、特に１つのコンテンツを特定の回数用いる事により、異なる利用条件での使用を可能にする方法について述べる。例えば、あるコンテンツを特定回数用いることで、より安い料金での使用を可能にするような方法である。

【００５０】また、本実施例は、本発明を特願平９－４１８号のユーザ認証技術に適用した例である。

【００５１】はじめに、本実施例で用いられるアクセスチケット（認証用補助情報）を用いた処理の概観を説明する。図６に処理の概観を示す。図６において、アクセスチケットを用いた処理は、チケット発行センタ３０と、コンテンツプロバイダ４０、及びユーザ環境５０から構成されるシステムにおいて実行される。

【００５２】チケット発行センタ３０は、チケット公開鍵データベース３１、ユーザデータベース３２、プロバイダデータベース３３及びアクセスチケット発行装置３４を持つ。コンテンツプロバイダ４０は、暗号化していないコンテンツと、慣用暗号鍵を保持し、慣用暗号装置よりコンテンツを暗号化する。

【００５３】また、ユーザ環境５０は、パソコンやワークステーションなど、ディジタル情報を利用するための情報処理装置である利用環境（ホスト）５１と、利用者の認証をするためにホスト５１に接続されているトークン５２とを含んでなる。ホスト５１はユーザツール５３およびカプセル化コンテンツ５４を含む。トークン５２は、各利用者に固有の情報を安全に封入したＩＣカードもしくはスマートカードのような耐タンパー容器であり、固有情報をもとに利用者の認証を行うための演算部を有している。トークン５２はあらかじめ各利用者に配布されている。

【００５４】はじめに、コンテンツプロバイダ４０は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｌｅｍａｎ）公開鍵の発行を、チケット発行センタ３０に対して要求する（①）。チケット発行センタ３０は要求に応じて、公開鍵をコンテンツプロバイダ４０に送付する（②）。コンテンツプロバイダ４０は自身で用意した慣用暗号鍵でコンテンツを暗号化し、その鍵をさらに発行された公開鍵で暗号化してコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（カプセル化コンテンツ）が、利用者（ユーザ環境）５０にネットワークやＣＤ－ＲＯＭなどを用いて配布される（③）。コンテンツは暗号化されているため、このままでは利用する事ができない。利用者は利用したいコンテンツ及び自分のユーザＩＤに対応したアクセスチケットの発行をセンタ３０に要求する（④）。アクセスチケットは、特定のコンテンツとユーザの固有情報がそろったときにのみ、そのコンテンツを利用可能にするためのディジタル情報であり、他のユーザとコンテンツの組み合わせでは使用できない。センタ３０はユーザの要求に応じてアクセスチケットを発行しユーザに送付する（⑤）。ユーザはアクセスチケットを用いてコンテンツを利用する。アクセスチケットにはアクセス制御のための情報以外に、利用料金や支払方法、使用期限などの利用条件に関する情報が付与されている。ユーザがコンテンツを利用すると、利用に応じてその履歴がトークン５２に記録される。この際、履歴にはその利用時点での利用条件も同時に記録される。ユーザは適当なタイミングで、センタ３０に利用履歴を送付する（⑥）。センタ３０は回収した利用履歴に基づいて課金を行う。回収した履歴に基づいて計算された料金が、それぞれの利用者の口座より引き落とされ、コンテンツプロバイダ４０に各コンテンツの利用量に応じて分配される（⑦）。

【００５５】次に、本実施例での処理を詳しく説明する。

【００５６】はじめに、コンテンツプロバイダ４０は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なＲＳＡ公開鍵ペアＥ，Ｄと法数ｎをセンタ３０より発行してもらう。コンテンツプロバイダ４０にはＥとｎが渡され、センタ３０は発行した公開鍵に対応する秘密鍵Ｄ、法数ｎを公開鍵データベース３１に記録して安全に管理しておく。次に、コンテンツプロバイダ３０は自身で用意した慣用暗号鍵Ｋによりこのコンテンツを暗号化する。さらに、このＫをセンタより発行された公開鍵Ｅで暗号化し、$K^* = K^E \mod n$を作成する。この$K^*$をコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（以下カプセル化コンテンツと呼ぶ）は、利用者にネットワークやＣＤ－ＲＯＭなどを用いて配布される。

【００５７】ユーザはコンテンツを利用するため、アクセスチケットの発行をセンタ３０に依頼する。図７にアクセスチケットの構成を示す。アクセスチケットは認証用情報（以下単にチケットと呼ぶ）ｔと、利用制限情報Ｌ、チケット法数ｎ、及び公開鍵Ｅからなる。アクセスチケットとコンテンツは一意に対応しており、コンテンツの公開鍵法数ｎによって対応関係を決定することができる。

【００５８】ここで、ある一定回数の利用後には異なった利用条件（例えば割引料金）での使用を可能にするため、アクセスチケットを発行する際に、センタ３０は以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では４種類の異なる利用条件を持つアクセスチケットとそれに対応する利用制限情報を用意する。

【００５９】

【数２】ｔ１＝Ｄ＋Ｆ（ｄｕ，Ｌ１，ｎ）
ｔ２＝Ｄ＋Ｆ（ｄｕ，Ｌ２，ｎ）
ｔ３＝Ｄ＋Ｆ（ｄｕ，Ｌ３，ｎ）
ｔ４＝Ｄ＋Ｆ（ｄｕ，Ｌ４，ｎ）

利用制限情報を図８に示す。

【００６０】上記の式および図８において、式「$(\alpha 1)^{FUr2(du,Ll,n)} \mod n$」は、α１をＦ（ｄｕ，Ｌ１，ｎ）でＵｒ２回べき乗し、ｎに関する剰余をとることを表す。ｔはチケット、Ｄはコンテンツの公開鍵に対応する秘密鍵、Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、ｄｕはユーザの秘密鍵、ｎはコンテンツの公開鍵法数、Ｉｒはチケット発行時に生成される乱数、Ｌは利用条件などを記した利用制限情報である。

【００６１】利用制限情報Ｌは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の１回の利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Ｌには、このアクセスチケットの使用順位、次のアクセスチケットを使用可能にするためのチケット活性化情報α、及び次のアクセスチケットが使用可能になるまでの回数Ｕｒが含まれている。

【００６２】チケット生成時には、ｔはＬを図８に示すように設定して計算される。すなわち、Ｕｒの値を全て０とし、αの計算にのみ実際のＵｒの値が用いられる。ｎ、Ｄの値はセンタ３０内の公開鍵データベース３１を、ｄｕの値はユーザデータベース３２を参照する事により得ることができる。

【００６３】ユーザにはｔ１からｔ４の一連のチケットと、利用制限情報Ｌ１～Ｌ４を含むアクセスチケットが配布される。但し、ユーザへの配布時にはＬ１～Ｌ４は、図９に示すようにＵｒ１～Ｕｒ４に値が設定され、さらにＬ２～Ｌ４のα２～α４の値を０としたものに置き換えられる。

【００６４】図１０にユーザ環境５０（図６）の構成を示す。ユーザ環境５０は利用環境（ホスト）５１とトークン５２からなり、トークン５２は証明情報演算部６４およびユーザ固有情報保持部６５を有している。ユーザ固有情報保持部６５には各ユーザに固有の情報が入れられている。固有情報はユーザには秘密であり、ユーザのＩＤとそれに対応する固有情報は、チケット発行センタ３０で安全に管理されている。

【００６５】利用環境（ホスト）５１は、カプセル化コンテンツ５４とユーザツール５３とを有する。ユーザツール５３は、アクセスチケット保持部（複数のチケット）５５、アクセスチケット検索部５６、および証明情報演算部５７を持つ。また、カプセル化コンテンツ５４には、乱数発生部５８、チケット公開鍵法数保持部５９、チケット公開鍵保持部６０、慣用暗号復号部６１、暗号化された慣用鍵の保持部６２、および暗号化コンテンツ保持部６３を有する。

【００６６】次に、ユーザ環境５０での処理について述べる。図１１および図１２にユーザ環境５０での処理を示す。ユーザ環境では以下の処理を行う。

［ステップＳ３１］　カプセル化コンテンツ５４が乱数ｒを生成する。

［ステップＳ３２］　カプセル化コンテンツ５４が$r^E K^E$ ｍｏｄ　ｎを計算し、この値とコンテンツの公開鍵法数ｎとをユーザツール５３に送付する。ｒを用いるのはトークンとの通信路上で慣用暗号鍵を知られるのを防ぐためである。

［ステップＳ３３］　ユーザツール５３が、管理しているチケット保持部５５から、ｎを法数として持つアクセスチケットを全て検索する。チケット保持部５５は、法数ｎと対応するチケットを組にして保持している。

［ステップＳ３４］　アクセスチケットが１つも見つからない場合は、処理を終了する。

［ステップＳ３５］　検索したチケットの中から、利用制限情報の残り使用回数Ｕｒが０のチケットで、最も使用順位の値が大きいものを選択する。

［ステップＳ３６］　現在のチケットと同じ法数ｎを持つチケットの中から、現在のチケットの次に使用順位の値が大きいチケットを検索する。

［ステップＳ３７、Ｓ３８、Ｓ３９］　チケットが見つかった場合、そのチケットの活性化情報の値を調べ、その値が０の場合には現在のチケットの活性化情報の値を書き込む。そして、$r^E K^E$ ｍｏｄ　ｎ，　法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。活性化情報がゼロでない場合はそのまま$r^E K^E$ ｍｏｄ　ｎ，法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。

［ステップＳ３６、Ｓ４０］　チケットが見つからない場合、αの値を０をとして、$r^E K^E$ ｍｏｄ　ｎ，ｎ，Ｌ、αの組みをトークン５２に送る。

［ステップＳ４１］　　トークン５２が、

【００６７】

【数３】$R1 = (r^E K^E)^{F(du,L,n)}$

$R2 = (\alpha)^{F(du,L,n)}$

を計算する。

［ステップＳ４２］　ユーザツール５３は、トークン５２が計算を行っている間に、$(r^E K^E)^t$の値を計算する。

［ステップＳ４３］　トークン５２は、計算したＲ１、Ｒ２の値をユーザツール５３に送る。

［ステップＳ４４～Ｓ４６］　次の使用順位のチケットがある場合には、ユーザツール５３は次のチケットの利用制限情報中の残り回数Ｕｒの値を１減らし、さらに、次のチケットの活性化情報フィールドの値を、Ｒ２の値で置き換える。

［ステップＳ４７］　トークン５２から受け取ったＲ１から、

$(r^E K^E)^t \cdot R1^{-1} = rK \mod n$

を計算してカプセル化コンテンツ５４に送付。

［ステップＳ４８］　カプセル化コンテンツ５４は、ｒＫよりＫを求める。ｒの値はカプセル化コンテンツ４９が発生させたものなので、Ｋの計算が可能である。

［ステップＳ４９］　カプセル化コンテンツ５４は、Ｋにより暗号化されたコンテンツ本体を慣用暗号復号部６１により復号して利用する。

【００６８】最初のチケットｔ１を１回使用した時点での、利用制限情報は図１３に示すようになる。

【００６９】ユーザがコンテンツを利用すると、その利用時点での利用条件がトークン５２に履歴として記録される。同じコンテンツであっても利用時点での利用条件での履歴が記録されるため、定まった利用順序・回数で定まった利用条件によるコンテンツの利用が可能になる。

【００７０】このようにチケットと利用制限情報の組を計算しておくことにより、例えば、第一のチケットｔ１を特定回数使うことで始めて、ｔ２の計算に用いられたＬ２中のα２を計算する事ができ、第二のチケットが利

用可能になる。第２のチケットの利用条件を第１のチケットと異なるものとすることで、例えば利用料金の割引などを行う事が可能になる。同様の処理により、順次異なった条件のチケットを、定まった順序・回数で利用する仕組みが実現できる。

【００７１】［実施例３］本実施例では特に、１つのコンテンツを特定の回数用いる事により、それとは異なったコンテンツの使用を定められた順番で可能にする方法について述べる。

【００７２】本実施例では実施例２と同様にアクセスチケットによる処理を行う。

【００７３】本実施例の構成は実施例２と同様であるが、アクセスチケットの利用制限情報に、使用順位の代わりに、次に使用可能となるコンテンツに対応する法数を入れるフィールドが追加される点が異なる。

【００７４】実施例の動作について説明する。

【００７５】実施例２と同様の方法により、コンテンツプロバイダ４０はセンタ３０から発行してもらった公開鍵を用いてコンテンツをカプセル化して配布する。ユーザは同様に、センタ３０に対してアクセスチケットの発行を要求する。

【００７６】ここで、あるコンテンツを特定回数利用した場合のみ、それとは異なるコンテンツを定まった順番で利用できるようにするため、アクセスチケットを発行する際に、センタは以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では４種類の異なったコンテンツと、それぞれのコンテンツに対応するアクセスチケットとそれに対応する利用制限情報（図１４）を用意する。

【００７７】アクセスチケットは次式のようなものである。

【００７８】

【数４】ｔ１＝Ｄ１＋Ｆ（ｄｕ，Ｌ１，ｎ１）
ｔ２＝Ｄ２＋Ｆ（ｄｕ，Ｌ２，ｎ２）
ｔ３＝Ｄ３＋Ｆ（ｄｕ，Ｌ３，ｎ３）
ｔ４＝Ｄ４＋Ｆ（ｄｕ，Ｌ４，ｎ４）

利用制限情報は図１４に示すようなものである。

【００７９】上記の式および図１４において式「$(\alpha 1)^{FUr2(du,LI,n2)}$　ｍｏｄ　ｎ」は、α１をＦ（ｄｕ，Ｌ１，ｎ２）でＵｒ２回べき乗し、ｎに関する剰余をとることを表す。ｔはチケット、Ｄはコンテンツの公開鍵に対応する秘密鍵、Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、ｄｕはユーザの秘密鍵、ｎはコンテンツの公開鍵法数、Ｉｒはチケット発行時に生成される乱数、Ｌは利用条件などを記した利用制限情報である。

【００８０】利用制限情報Ｌは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の１回の



利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Ｌには、次のアクセスチケットを使用可能にするためのチケット活性化情報α、次のアクセスチケットが使用可能になるまでの回数Ｕｒ、および次に使用可能になるチケットの法数が含まれている。

【００８１】チケット生成時には、ｔはＬを上記の表のように設定して計算される。すなわち、Ｕｒの値を全て０とし、αの計算にのみ実際のＵｒの値が用いられる。

【００８２】ユーザにはｔ１からｔ４の一連のチケットと、利用制限情報Ｌ１～Ｌ４を含むアクセスチケットが配布される。但し、ユーザへの配布時にはＬ１～Ｌ４は、図１５に示すようにＵｒ１～Ｕｒ４に値が設定され、さらにＬ２～Ｌ４のα２～α４の値を０としたものに置き換えられる。

【００８３】次に、ユーザ環境での処理について述べる。ユーザ環境５０の構成は実施例２と同様である。図１６および図１７にユーザ環境５０での処理を示す。ユーザ環境５０では以下の処理を行う。

［ステップＳ５１］　カプセル化コンテンツ５４が乱数ｒを生成する。

［ステップＳ５２］　カプセル化コンテンツ５４は$r^E K^E$　ｍｏｄ　ｎを計算し、この値とコンテンツの公開鍵法数ｎをユーザツール５３に送付する。ｒを用いるのはトークン５２との通信路上で慣用暗号鍵を知られるのを防ぐためである。

［ステップＳ５３］　ユーザツール５３は、管理しているチケット保持部５５から、ｎを法数として持つチケットを検索する。チケット保持部５５は、法数ｎと対応するチケットを組にして保持している。

［ステップＳ５４］　チケットが見つからなかった場合は処理を終了する。

［ステップＳ５５］　検索したチケットの残り利用回数Ｕｒが０でなければ、そのチケットはまだ有効ではないので、処理を終了する。

［ステップＳ５６］　ユーザツール５３は現在のチケットの利用制限情報Ｌの、次のチケットの法数の値を調べる。

［ステップＳ５７～Ｓ６０］　法数の値が０ではなく、この法数に対応する次のチケットが存在する場合、そのチケットの活性化情報の値を調べ、その値が０の場合には現在のチケットの活性化情報の値を書き込む。

［ステップＳ６１］　さらに$r^E K^E$　ｍｏｄ　ｎ，法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。

［ステップＳ６２］　次のチケットの法数の値が０か、法数の示すチケットが存在しない場合には、、αの値を０をとして、$r^E K^E$　ｍｏｄ　ｎ，ｎ，Ｌ，αの組みをトークン５２に送る。

［ステップＳ６３］　トークン５２は

17

【００８４】
【数５】Ｒ１＝（$r^E K^E$）$^{F(du,L,n)}$　、
Ｒ２＝（$\alpha$）$^{F(du,L,n)}$
を計算する。
［ステップＳ６４］　ユーザツール５３はトークン５２が計算を行っている間に、（$r^E K^E$）$^t$の値を計算する。
［ステップＳ６５］　トークン５２は、計算したＲ１、Ｒ２の値をユーザツール５３に送る。
［ステップＳ６６～Ｓ６８］　次のチケットがある場合には、ユーザツール５３は、次のチケットの利用制限情報中の残り回数Ｕｒの値を１減らし、さらに、次のチケットの活性化情報フィールドの値を、Ｒ２の値で置き換える。
［ステップＳ６９］　トークン５２から受け取ったＲ１から、
【００８５】
【数６】（$r^E K^E$）$^t$・$R1^{-1}$＝ｒＫ　ｍｏｄ　ｎ
を計算してカプセル化コンテンツ５４に送付する。
［ステップＳ７０］　カプセル化コンテンツ５４は、ｒＫよりＫを求める。ｒの値はカプセル化コンテンツ５４が発生させたものなので、Ｋの計算が可能である。
［ステップＳ７１］　カプセル化コンテンツ５４は、Ｋにより暗号化されたコンテンツ本体を慣用暗号復号部６１により復号して利用する。
【００８６】最初のチケットｔ１を１回使用した時点での、利用制限情報は図１８に示すようになる。
【００８７】実施例２と同様の方法により、ユーザの利用に応じて利用履歴がトークン５２に記録され、これをセンタ３０が回収する事により、利用者への課金とコンテンツプロバイダ４０への料金の分配が行われる。
【００８８】このようにチケットと利用制限情報の組をあらかじめ計算して配布することにより、例えば、第一のチケットｔ１を特定回数使うことで始めて、ｔ２の計算に用いられたＬ２中の$\alpha$２を計算する事ができ、第二のチケットが利用可能になる。第２のチケットには異なるコンテンツが対応づけられており、これにより、定まった順序で次のコンテンツを使用させる事ができる。同様の処理により、順次異なったコンテンツを、あらかじめ定められた順序でのみ利用させる仕組みが実現できる。
【００８９】また、本実施例の変形として、２つのアクセスチケットを１回ずつ利用する事で、はじめて他のチケットを使用可能にするような仕組みも実現可能である。そのために、センタは以下のようなチケットと利用制限情報を用意する。
【００９０】アクセスチケットは次のようなものである。
【００９１】
【数７】ｔ１＝Ｄ１＋Ｆ（ｄｕ，Ｌ１，ｎ１）

18

ｔ２＝Ｄ２＋Ｆ（ｄｕ，Ｌ２，ｎ２）
ｔ３＝Ｄ３＋Ｆ（ｄｕ，Ｌ３，ｎ３）
利用制限情報は図１９に示すようなものである。
【００９２】上記の式および図１９において、Ｉｒ１、Ｉｒ２はチケット発行時に生成される乱数、Ｎはこのチケットを活性化させるのに必要な活性化情報の数である。また、ｆは使用履歴を示すフラグで、１度使われるとこの値は１に書き換えられる。
【００９３】ユーザにはｔ１からｔ３の一連のチケットと、利用制限情報Ｌ１～Ｌ３を含むアクセスチケットが配布される。但し、ユーザへの配布時には図２０に示すように、Ｌ３は、$\alpha$３の値を０としたものに置き換えられる。
【００９４】ｔ１、ｔ２を最初に使用すると、それぞれの使用履歴が１に書き換えられるとともに、ｔ３のための活性化情報
【００９５】
【数８】$\alpha 1' = \alpha 1^{F(du,L1,n1)}$
$\alpha 2' = \alpha 2^{F(du,L2,n2)}$
が計算されて、Ｌ３に保持される。ｔ３を使用する際に、Ｎ３個の必要な活性化情報がそろっていた場合には、
【００９６】
【数９】$\alpha 3 = \alpha 1' + \alpha 2' = \alpha 1^{F(du,L1,n1)} + \alpha 2^{F(du,L2,n2)}$
が計算できるので、ｔ３の使用が可能になる。
【００９７】このようにすることで、ｔ１、ｔ２の利用の順番を特定せずに、両方のチケットを使ったときのみ、ｔ３が有効になる仕組みを実現できる。
【００９８】
【発明の効果】以上のように、本発明を用いる事で、オフライン環境下においても、ユーザ環境および提供するコンテンツそのものに特段の機構を追加することなく、また、センタとのコンテンツの利用毎の通信を伴うこともなしに、暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御が可能になる。
【図面の簡単な説明】
【図１】　本発明の実施例１の構成を示すブロック図である。
【図２】　実施例１の処理を説明するフローチャートである。
【図３】　実施例１の処理を説明するフローチャートである。
【図４】　実施例１の鍵保持部の構造（初期値）を示す図である。
【図５】　実施例１の鍵保持部の構造（２番目の鍵Ｋ２が使用可能になった状態）を示す図である。
【図６】　本発明の実施例２で用いるアクセスチケットによる処理を説明する図である。
【図７】　アクセスチケットの構成を示す図である。

【図８】　実施例２の利用制限情報を説明する図である。

【図９】　実施例２の利用制限情報（ユーザに当初送られるもの）を説明する図である

【図１０】　実施例２のユーザ環境の構成を示すブロック図である。

【図１１】　実施例２の動作を説明するためのフローチャートである。

【図１２】　実施例２の動作を説明するためのフローチャートである。

【図１３】　実施例２の利用制限情報（最初のチケットを１回利用した後のもの）を説明する図である。

【図１４】　本発明の実施例３の利用制限情報を説明する図である。

【図１５】　実施例３の利用制限情報（ユーザに当初送られるもの）を説明する図である。

【図１６】　実施例３の動作を説明するフローチャートである。

【図１７】　実施例３の動作を説明するフローチャートである。

【図１８】　実施例３の利用制限情報（最初のチケットを１回利用した後のもの）を説明する図である。

【図１９】　実施例３の変形例の利用制限情報を説明する図である。

【図２０】　上述変形例の利用制限情報（ユーザに当初送られるもの）を説明する図である。

【符号の説明】

１０　利用環境（ホスト）
１１　暗号化コンテンツ保持部
１２　鍵保持部
２０　トークン
２１　鍵活性化情報演算部
２２　慣用暗号復号部２２

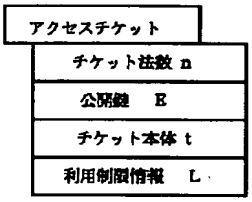
【図４】

| 鍵ID | 鍵 | 次の鍵ID | 鍵活性化情報 | 使用可能になるまでの回数 |
|---|---|---|---|---|
| $I_1$ | $K_1$ | $I_2$ | 0 | 0 |
| $I_2$ | $K_2'$ | $I_3$ | 0 | Ur2 |
| $I_3$ | $K_3'$ | $I_4$ | 0 | Ur3 |
| $I_4$ | $K_4'$ | 0 | 0 | Ur4 |

【図５】

| 鍵ID | 鍵 | 次の鍵ID | 鍵活性化情報 | 使用可能になるまでの回数 |
|---|---|---|---|---|
| $I_1$ | $K_1$ | $I_2$ | $\alpha_1'=F^{Ur2-1}(\alpha_1)$ | 0 |
| $I_2$ | $K_2=K_2'+F(\alpha_1')$ | $I_3$ | 0 | 0 |
| $I_3$ | $K_3'$ | $I_4$ | 0 | Ur3 |
| $I_4$ | $K_4'$ | 0 | 0 | Ur4 |

【図７】



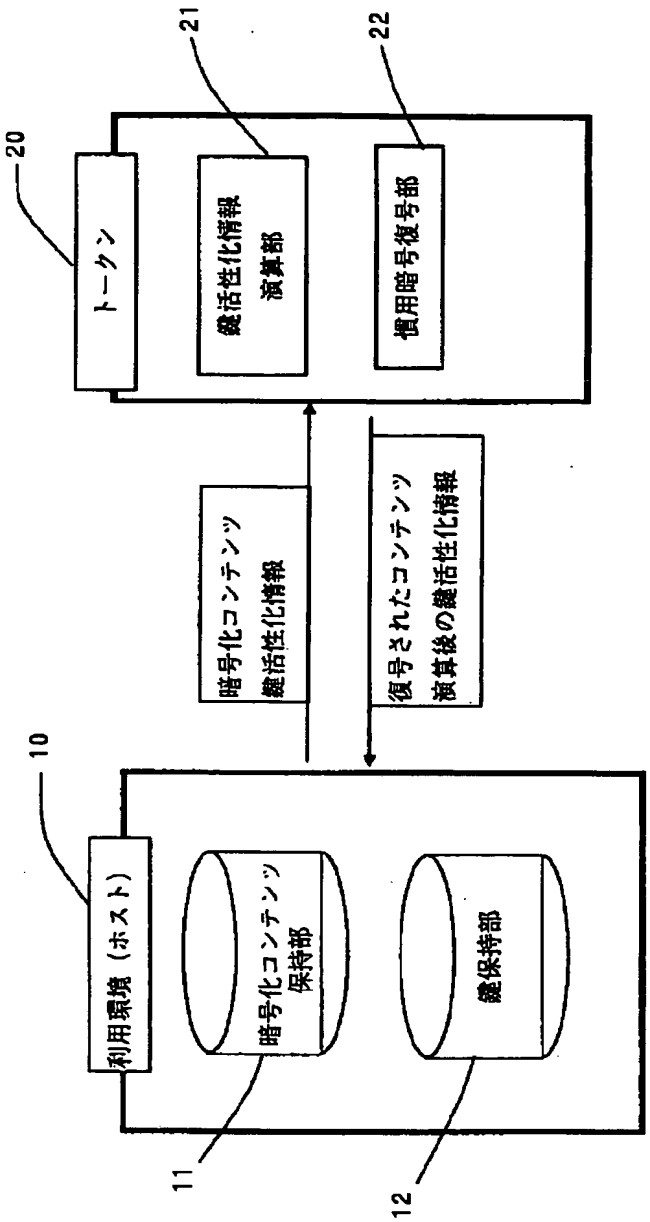

【図９】

| 利用制限情報 | 使用期限 | 利用料金 | 使用順位 | 使用可能になるまでの回数 | チケット活性化情報 |
|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | 1 | Ur1=0 | $\alpha_1=I_r$ |
| $L_2$ | 1997/12/31 | 80 | 2 | Ur2=20 | $\alpha_2=0$ |
| $L_3$ | 1997/12/31 | 60 | 3 | Ur3=20 | $\alpha_3=0$ |
| $L_4$ | 1997/12/31 | 40 | 4 | Ur4=20 | $\alpha_4=0$ |

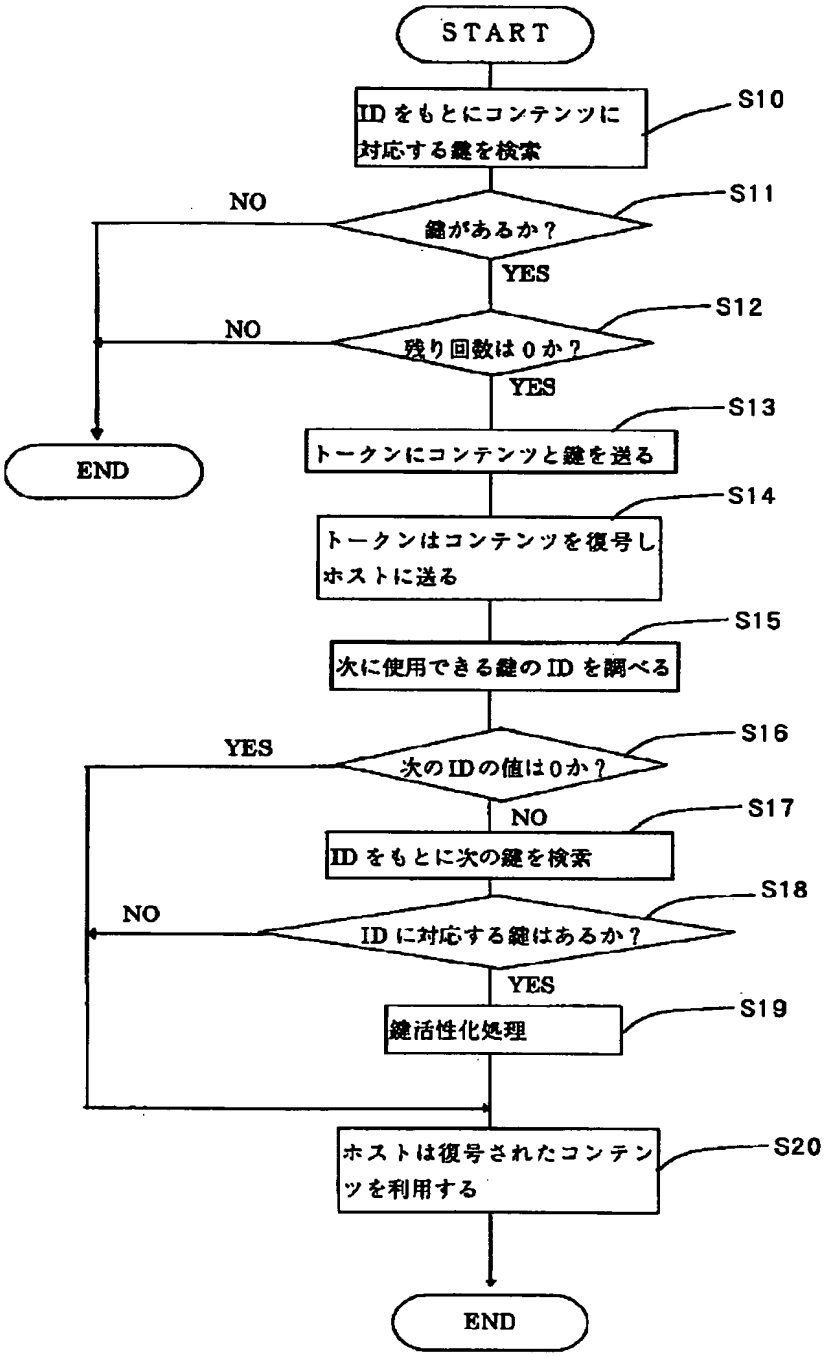
【図１３】

| 利用制限情報 | 使用期限 | 利用料金 | 使用順位 | 使用可能になるまでの回数 | チケット活性化情報 |
|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | 1 | Ur1=0 | $\alpha_1=I_r$ |
| $L_2$ | 1997/12/31 | 80 | 2 | Ur2=19 | $\alpha_2=(\alpha_1)^{F(a,L_2,n)} \bmod n$ |
| $L_3$ | 1997/12/31 | 60 | 3 | Ur3=20 | $\alpha_3=0$ |
| $L_4$ | 1997/12/31 | 40 | 4 | Ur4=20 | $\alpha_4=0$ |

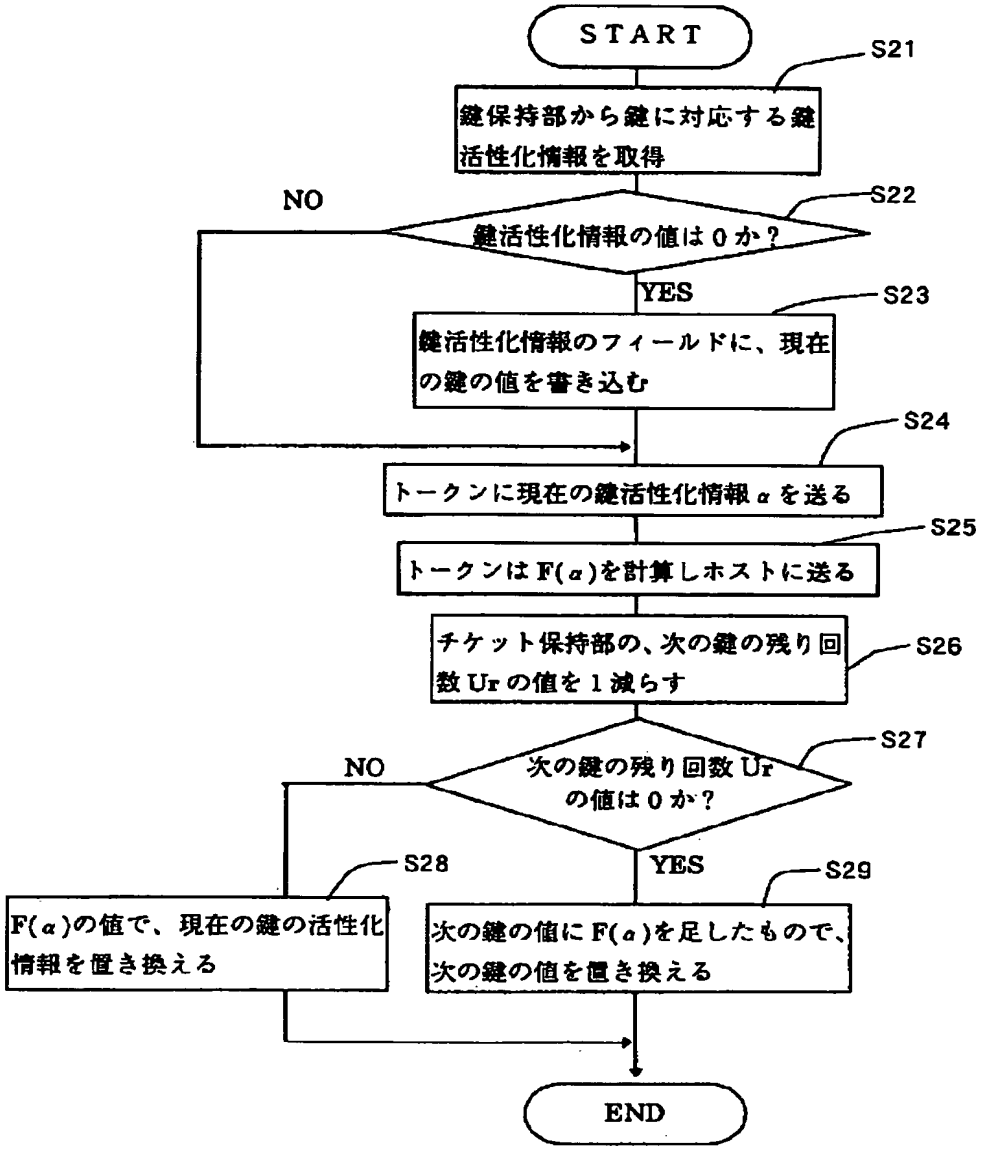
【図１】


20
21
22
トークン
鍵活性化情報
演算部
慣用暗号復号部
暗号化コンテンツ
鍵活性化情報
復号されたコンテンツ
演算後の鍵活性化情報
10
利用環境（ホスト）
暗号化コンテンツ
保持部
鍵保持部
11
12

【図２】


START
IDをもとにコンテンツに対応する鍵を検索
S10
鍵があるか？
S11
NO
YES
残り回数は0か？
S12
NO
YES
END
トークンにコンテンツと鍵を送る
S13
トークンはコンテンツを復号しホストに送る
S14
次に使用できる鍵のIDを調べる
S15
次のIDの値は0か？
S16
YES
NO
IDをもとに次の鍵を検索
S17
IDに対応する鍵はあるか？
S18
NO
YES
鍵活性化処理
S19
ホストは復号されたコンテンツを利用する
S20
END

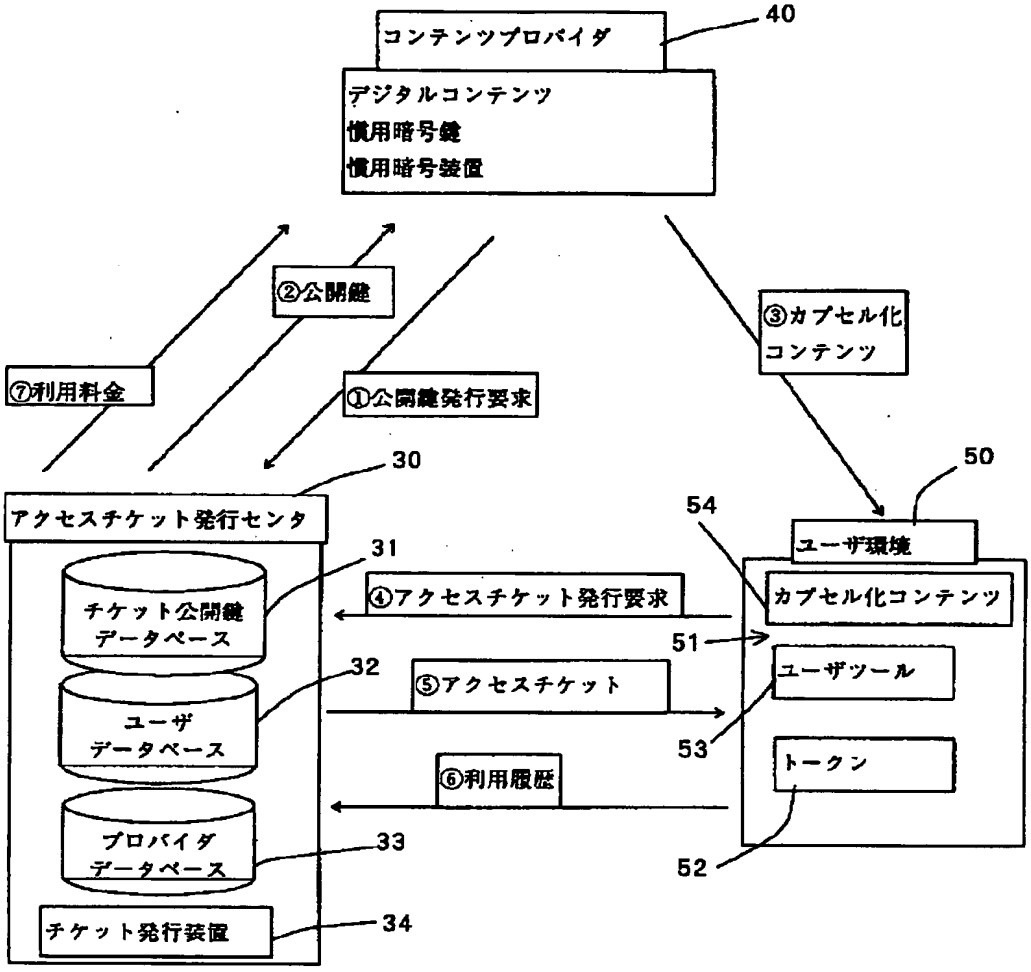
【図３】




【図１９】

| 利用制限情報 | 使用期限 | 利用料金 | 次のチケットの枚数 | 使用履歴を示すフラグf | 必要な活性化情報の数 | チケット活性化情報α |
|---|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | $n_2$ | 0 | $N_1=1$ | $\alpha_1=I_{T1}$ |
| $L_2$ | 1997/12/31 | 100 | $n_3$ | 0 | $N_2=1$ | $\alpha_2=I_{T2}$ |
| $L_3$ | 1997/12/31 | 100 | 0 | 0 | $N_3=2$ | $\alpha_3=\alpha_1^{F(\alpha_2,L_3,0)}+\alpha_2^{F(\alpha_1,L_3,0)}$ |

【図６】




【図１４】

| 利用制限情報 | 使用期限 | 利用料金 | 次のチケットの法数 | 使用可能になるまでの回数 $U_T$ | チケット活性化情報 $\alpha$ |
|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | $n_3$ | $U_{T1}=0$ | $\alpha_1=I_T$ |
| $L_2$ | 1997/12/31 | 100 | $n_3$ | $U_{T2}=0$ | $\alpha_2=(\alpha_1)^{PU_{T2}(n_3,L_2,n_2)} \bmod n$ : $U_{T2}=20$ |
| $L_3$ | 1997/12/31 | 100 | $n_4$ | $U_{T3}=0$ | $\alpha_3=(\alpha_2)^{PU_{T3}(n_4,L_3,n_3)} \bmod n$ : $U_{T3}=20$ |
| $L_4$ | 1997/12/31 | 100 | 0 | $U_{T4}=0$ | $\alpha_4=(\alpha_3)^{PU_{T4}(n_5,L_4,n_4)} \bmod n$ : $U_{T4}=20$ |

【図８】

| 利用制限情報 | 使用期限 | 利用料金 | 使用順位 | 使用可能になるまでの回数 Ur | チケット活性化情報 $\alpha$ |
|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | 1 | Ur1=0 | $\alpha_1=Ir$ |
| $L_2$ | 1997/12/31 | 80 | 2 | Ur2=0 | $\alpha_3=(\alpha_1)^{F^{Ur2}(du,L_1,n)} \bmod n$ : Ur2=20 |
| $L_3$ | 1997/12/31 | 60 | 3 | Ur3=0 | $\alpha_3=(\alpha_2)^{F^{Ur3}(du,L_2,n)} \bmod n$ : Ur3=20 |
| $L_4$ | 1997/12/31 | 40 | 4 | Ur4=0 | $\alpha_4=(\alpha_3)^{F^{Ur4}(du,L_3,n)} \bmod n$ : Ur4=20 |

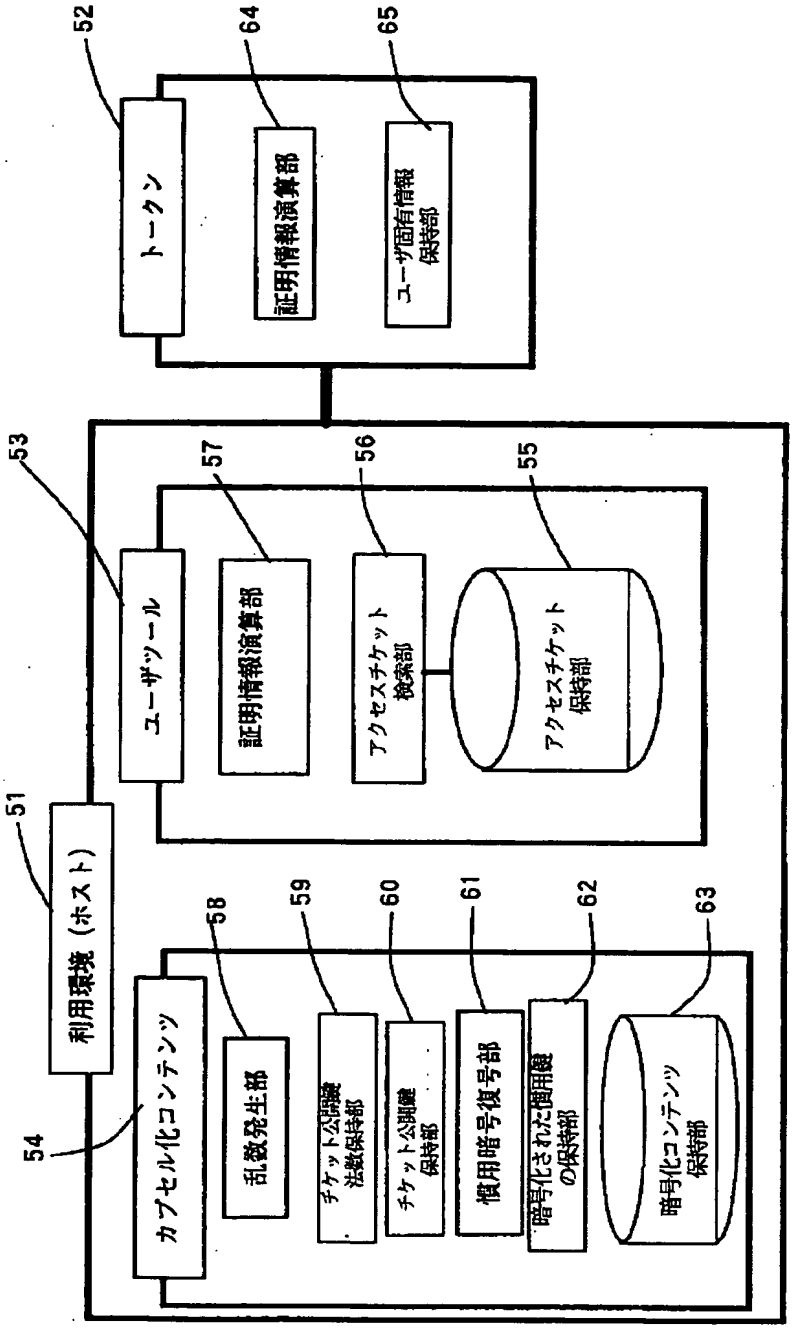
【図１５】

| 利用制限情報 | 使用期限 | 利用料金 | 次のチケットの法数 | 使用可能になるまでの回数 | チケット活性化情報 |
|---|---|---|---|---|---|
| $L_A$ | 1997/12/31 | 100 | $n_B$ | Ur1=0 | $\alpha_1=Ir$ |
| $L_B$ | 1997/12/31 | 100 | $n_3$ | Ur2=20 | $\alpha_2=0$ |
| $L_3$ | 1997/12/31 | 100 | $n_4$ | Ur3=20 | $\alpha_3=0$ |
| $L_4$ | 1997/12/31 | 100 | 0 | Ur4=20 | $\alpha_4=0$ |

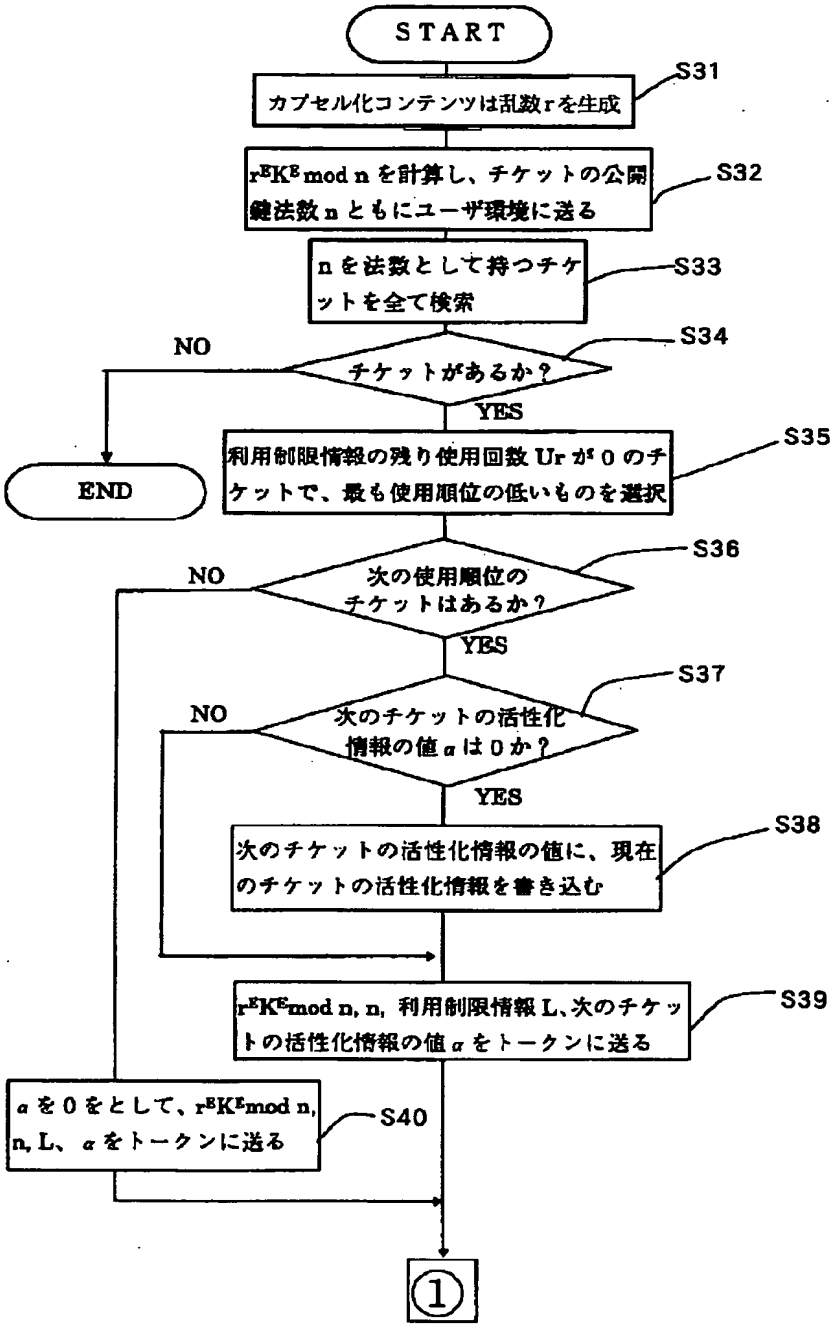
【図２０】

| 利用制限情報 | 使用期限 | 利用料金 | 次のチケットの法数 | 使用履歴を示すフラグf | 必要な活性化情報の数 | チケット活性化情報 $\alpha$ |
|---|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | $n_2$ | 0 | $N_1=1$ | $\alpha_1=Ir_1$ |
| $L_2$ | 1997/12/31 | 100 | $n_3$ | 0 | $N_2=1$ | $\alpha_2=Ir_2$ |
| $L_3$ | 1997/12/31 | 100 | 0 | 0 | $N_3=2$ | $\alpha_3=0$ |

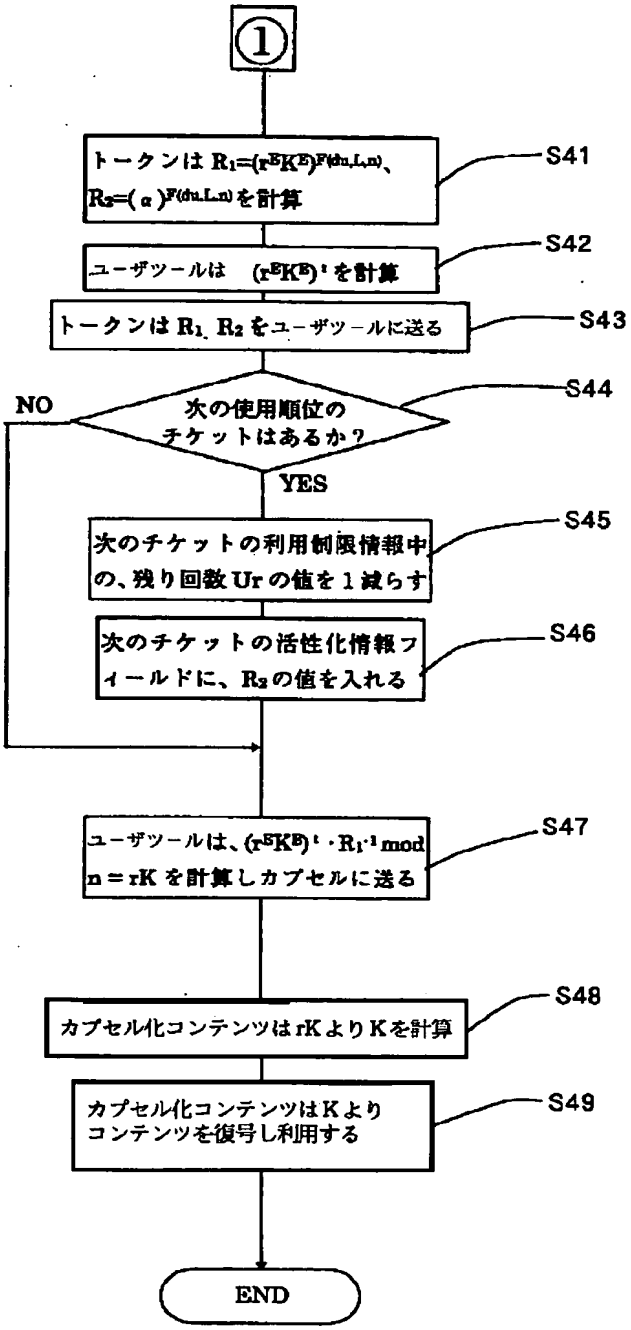
【図１０】


52
64
65
トークン
証明情報演算部
ユーザ固有情報保持部
53
57
56
55
ユーザツール
証明情報演算部
アクセスチケット検索部
アクセスチケット保持部
51
利用環境（ホスト）
58
59
60
61
62
63
54
カプセル化コンテンツ
乱数発生部
チケット公開鍵法数保持部
チケット公開鍵保持部
慣用暗号復号部
暗号化された慣用鍵の保持部
暗号化コンテンツ保持部

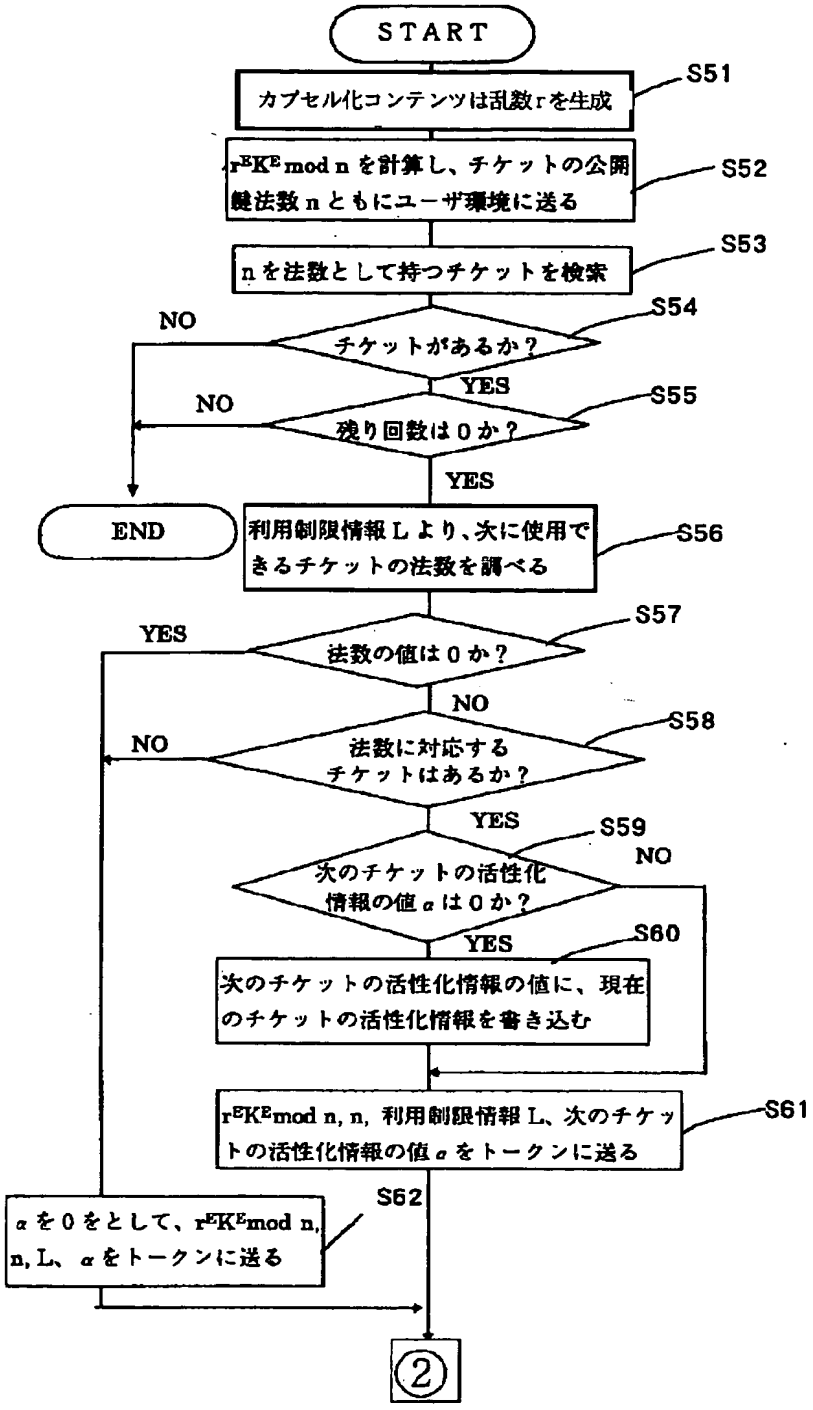
【図１１】


START
S31
カプセル化コンテンツは乱数rを生成
S32
$r^E K^E \bmod n$ を計算し、チケットの公開鍵法数nともにユーザ環境に送る
S33
nを法数として持つチケットを全て検索
S34
チケットがあるか？
NO
YES
END
S35
利用制限情報の残り使用回数Urが０のチケットで、最も使用順位の低いものを選択
S36
次の使用順位のチケットはあるか？
NO
YES
S37
次のチケットの活性化情報の値αは０か？
NO
YES
S38
次のチケットの活性化情報の値に、現在のチケットの活性化情報を書き込む
S39
$r^E K^E \bmod n$, n, 利用制限情報L、次のチケットの活性化情報の値αをトークンに送る
S40
αを０をとして、$r^E K^E \bmod n$, n, L、αをトークンに送る
①

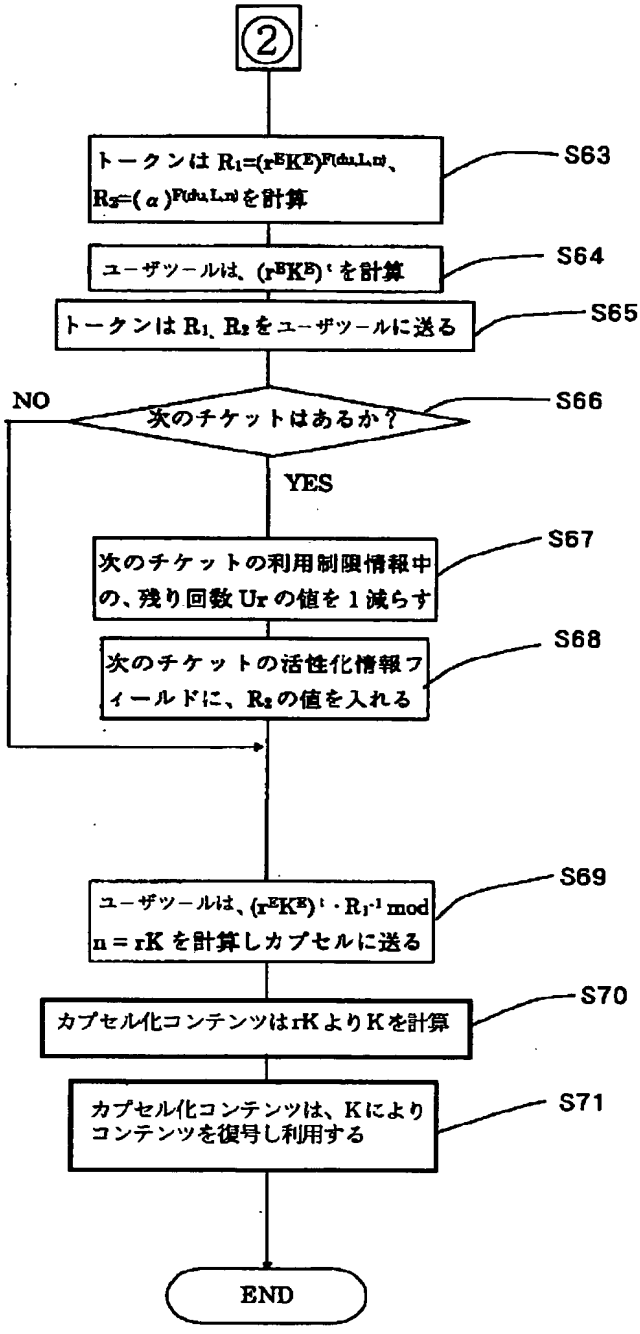
【図１２】


①
トークンは $R_1=(r^E K^E)^{F(du,L,n)}$、$R_2=(\alpha)^{F(du,L,n)}$を計算
S41
ユーザツールは　$(r^E K^E)^{-1}$を計算
S42
トークンは $R_1$、$R_2$をユーザツールに送る
S43
次の使用順位のチケットはあるか？
S44
NO
YES
次のチケットの利用制限情報中の、残り回数Urの値を１減らす
S45
次のチケットの活性化情報フィールドに、$R_2$の値を入れる
S46
ユーザツールは、$(r^E K^E)^{-1} \cdot R_1^{-1} \bmod n = rK$を計算しカプセルに送る
S47
カプセル化コンテンツはrKよりKを計算
S48
カプセル化コンテンツはKよりコンテンツを復号し利用する
S49
END

【図１６】


START
カプセル化コンテンツは乱数rを生成
S51
$r^E K^E \bmod n$ を計算し、チケットの公開鍵法数nともにユーザ環境に送る
S52
nを法数として持つチケットを検索
S53
チケットがあるか？
S54
NO
YES
残り回数は０か？
S55
NO
YES
END
利用制限情報Lより、次に使用できるチケットの法数を調べる
S56
法数の値は０か？
S57
YES
NO
法数に対応するチケットはあるか？
S58
NO
YES
次のチケットの活性化情報の値αは０か？
S59
NO
YES
次のチケットの活性化情報の値に、現在のチケットの活性化情報を書き込む
S60
$r^E K^E \bmod n$, n, 利用制限情報L、次のチケットの活性化情報の値αをトークンに送る
S61
αを０をとして、$r^E K^E \bmod n$, n, L、αをトークンに送る
S62
②

【図１７】


②
トークンは $R_1=(r^E K^E)^{F(du,L,n)}$、$R_2=(\alpha)^{F(du,L,n)}$を計算
S63
ユーザツールは、$(r^E K^E)^t$を計算
S64
トークンは $R_1$、$R_2$をユーザツールに送る
S65
NO
次のチケットはあるか？
S66
YES
次のチケットの利用制限情報中の、残り回数 Ur の値を１減らす
S67
次のチケットの活性化情報フィールドに、$R_2$の値を入れる
S68
ユーザツールは、$(r^E K^E)^t \cdot R_1^{-1} \bmod n = rK$を計算しカプセルに送る
S69
カプセル化コンテンツはrKよりKを計算
S70
カプセル化コンテンツは、Kによりコンテンツを復号し利用する
S71
END

【図１８】

| 利用制限情報 | 使用期限 | 利用料金 | 次のチケットの枚数 | 使用可能になるまでの回数 | チケット活性化情報 |
|---|---|---|---|---|---|
| $L_1$ | 1997/12/31 | 100 | $n_2$ | $U_{r1}=0$ | $e_1=I_r$ |
| $L_2$ | 1997/12/31 | 100 | $n_3$ | $U_{r2}=19$ | $e_2=(e_1)^{P_{1a},L_{1,n2}} \bmod n$ |
| $L_3$ | 1997/12/31 | 100 | $n_4$ | $U_{r3}=20$ | $e_3=0$ |
| $L_4$ | 1997/12/31 | 100 | 0 | $U_{r4}=20$ | $e_4=0$ |

フロントページの続き

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| // Ｇ０６Ｆ　12/14 | ３２０ | Ｈ０４Ｌ　9/00 | ６０１Ｅ |
| | | | ６４１ |